CLAIMS

What is claimed is:

1. A method of reconstructing a session using a first analyzer coupled to a second analyzer and a data collector, the method comprising:

performing session reconstruction analysis on packets received at the first analyzer;

responsive to successful session reconstruction on the first analyzer, sending a first message to at least one of the second analyzer and the data collector, the first message corresponding to session data; and

responsive to unsuccessful session reconstruction on the first analyzer, sending one or more messages to the second analyzer, the second analyzer also receiving one or more messages from a third analyzer.

2. The method of claim 1, wherein the one or more messages from the first analyzer to the second analyzer comprise packets received by the first analyzer.

3. The method of claim 2, wherein the one or more messages from the first analyzer to the second analyzer further comprise hints generated by the first analyzer.

4. The method of claim 3, wherein hints for a packet comprise a time the packet was received and an address information for the packet.

5. The method of claim 1, wherein the packets received at the first analyzer are output from a filter for controlling which packets in a plurality of packets flowing into the filter reach the first analyzer.

6. The method of claim 1, further comprising:

performing session reconstruction analysis on the one or more messages received at the second analyzer;

responsive to successful session reconstruction on the second analyzer, sending a first message to at least one of a fourth analyzer and the data collector, the first message corresponding to session data; and

responsive to unsuccessful session reconstruction on the second analyzer, sending one or more messages to the fourth analyzer, the fourth analyzer also receiving one or more messages from a fifth analyzer.

7. The method of claim 1, wherein the one or more messages from the first analyzer to the second analyzer comprise summary of packets received by the first analyzer and one or more hints generated by the first analyzer.

8. The method of claim 1, further comprising performing session reconstruction using the second analyzer on the one or more messages received from the first analyzer and the one or more messages received from the third analyzer.

9. The method of claim 8, further comprising sending a second message from the second analyzer to the data collector, the second message corresponding to session data.

10. A system for reconstructing a session, the system comprising:

a plurality of packet sources, each of the plurality of packet sources generating a plurality of packets;

a first analyzer;

a plurality of analyzers, each of the plurality of analyzers coupled to a packet source in the plurality of packet sources, each of the plurality of analyzers for session reconstruction on respective packets in the corresponding packet source, each of the plurality of analyzers sending a first message corresponding to session data for reconstructed sessions to the first analyzer and a second message for unreconstructed session data in the respective packets to the first analyzer, and wherein the first analyzer responsive to receiving messages from the plurality of analyzers attempts session reconstruction using the messages.

11. The system of claim 10 wherein the second message comprises respective packets.

12. The system of claim 11 wherein the second message further comprises hints.

13. The system of claim 10 wherein the second message comprises summary of respective packets and hints.